

## REMARKS

Upon entry of the present amendment, claims 1, 9 and 10 will be amended, and claims 28-31 will be newly added. Claims 1-31 will remain pending in the present application. Claims 1, 10, 15 and 21 are independent claims.

Applicant respectfully submits that the amendments to the claims are fully supported by the original disclosure, and introduce no new matter therewith. Applicant requests reconsideration and allowance in view of the foregoing amendments and the following remarks.

Entry of this Amendment is proper under 37 C.F.R. § 116 because the amendments: (a) place the application in condition for allowance for the reasons discussed herein; (b) do not raise any new issues that would require further consideration and/or search as the amendments and arguments presented merely amplify issues previously discussed throughout prosecution; and (c) place the application in better form for an appeal, should an appeal be necessary. The amendments are necessary and were not earlier presented as they are in response to new grounds of rejection entered in the Final Rejection. Applicant respectfully requests entry of the Amendment.

### *New Power of Attorney and Attorney Docket Number*

1. Applicant submitted a Form PTO/SB/82, a Form PTO/SB/96, and copies of associated Assignment documents to change of the Power of Attorney and the Attorney Docket Number on June 27, 2005. Applicant subsequently requested entry of the Power of Attorney in

the Amendment filed November 14, 2005. However, the Office has apparently not changed the Power of Attorney or the Attorney Docket Number because the Office Action mailed December 28, 2005 was mailed to the previous Power of Attorney and included the previous Attorney Docket Number. In order to expedite change of the Power of Attorney and the Attorney Docket Number, Applicant has submitted herewith another Form PTO/SB/82 and Form PTO/SB/96. Applicant respectfully requests that the Office change the Power of Attorney and the Attorney Docket Number accordingly.

***Premature Final Rejection***

2. Applicant respectfully submits that the Final Rejection mailed December 28, 2005 is premature and should be withdrawn. Applicant has previously filed Amendments June 25, 2005 and November 14, 2005 in response to Office Actions mailed February 25, 2005 and July 25, 2005, respectively. The Office has applied additional prior art in response to Applicant's Amendments and arguments. In the Final Rejection mailed December 28, 2005, the Office changed the grounds of rejection by applying Ober and pages 166 and 167 of Schneier. Ober was previously cited with the Office Action mailed February 25, 2005, and was applied to allegedly address the three different keys in the claims. Pages 166, 167 and previously cited page 177 of Schneier were applied to allegedly address the lengths of the encrypting keys.

Applicant respectfully submits that three different keys have been recited in the claims using different names since the initial filing of the present Application. When a new ground of

rejection is made by the Examiner that is not necessitated by Applicant's amendment of the claims, the rejection may not be made final. See MPEP § 706.07(a) and MPEP § 2144.03 D.

Applicant respectfully requests reconsideration and withdrawal of the Final Rejection mailed December 28, 2005.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold and Fischer***

3. Claims 1-9 and 15-18 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924) and Fischer (U.S. Patent No. 6,141,423). Applicant respectfully traverses this rejection.

Amended claim 1 recites a method for transferring a first root key between a key provider system and a second other system via an information network. The method includes the steps of a) encrypting the first root key using a first super-root key of the key provider system; b) providing within the second other system a first secure module having a second super-root key within a read-only memory circuit thereof and provided with the first secure module, the second super-root key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second super-root key is other than modifiable and other than accessible outside of the module; c) transferring the encrypted first root key from the key provider system to the second other system via the information network; d) providing the encrypted first root key to the processor internal to the first secure module of the second other

system; and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored within the read-only memory circuit of the first secure module and to store the decrypted first root key internally within a secure key memory location of the first secure module, wherein the first root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the first root key, and the bit length of the first root key is greater than a bit length of any of the private keys.

Claim 15 recites a system for transferring a secure root key between a key provider system and a second other system via an information network that is other than secure including a secure module in operative communication with the second other system. The secure module includes an encryption processor, an input port, a memory circuit, and memory storage. The input port is for receiving encrypted electronic data from outside the module and for providing the encrypted electronic data to the encryption processor. The memory circuit is in operative communication with the encryption processor for storing at least a first super-root key. The memory storage has program code stored therein and executable on the encryption processor for, upon receipt of an encrypted secure root key, decrypting the encrypted secure root key using the at least a first super-root key and for storing the decrypted secure root key within the memory circuit, the at least a first super-root key being other than accessible by any code other than the program code and being other than modifiable thereby, wherein the secure root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first

super-root key is greater than a bit length of the secure root key, and the bit length of the secure root key is greater than a bit length of any of the private keys.

Applicant respectfully submits that for at least the following two reasons, the combined teachings of Schneier, Ober, Arnold and Fischer do not establish a *prima facie* case of obviousness to reject amended claim 1 and claim 15.

First, as previously argued, Schneier, Arnold and Fischer do not teach or reasonably suggest the claimed relationship between the "first root key," the "first super-root key," and the "private encryption keys." Specifically, Schneier, Arnold and Fischer do not teach or reasonably suggest "encrypting the first root key using a first super-root key of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the first root key is useable for at least one of encrypting and decrypting private keys," as recited in claim 1. Schneier only discloses two types of keys: Key-Encryption Keys and Data Keys, and therefore does not teach a relationship between three keys (see Schneier, page 176). Arnold only discloses two types of keys: the private key  $K_{PR}$  and the public key  $K_{PU}$ , and thus does not teach a relationship between three keys (see Arnold, col. 5, lines 31-38). Fischer discloses a private key, a random DES key, a public key, and a trustee's public key (see Fischer, col. 4, lines 59-61, col. 7, lines 28-33, col. 9, lines 58-60). However, Fischer does not teach or suggest encrypting the random DES key with the public key, transferring the encrypted random DES key to a key provider to a second system via an information network, and using the random DES key for encrypting and decrypting the

private key. Thus, Schneier, Arnold and Fischer do not teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claims 1 and 15.

Ober fails to supplement the deficiencies of Schneier, Arnold and Fischer because Ober does not teach or reasonably suggest not teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claims 1 and 15.

Second, the Office has improperly applied individual parts of Schneier, Ober, Arnold and Fischer as a mosaic to recreate a facsimile of the invention. It is well known that it is improper to use the claims as a frame, and use individual parts of prior art as a mosaic to recreate a facsimile of the invention. *Interconnect Planning Corp. v. Feil*, 227 USPQ 2d 543, 551 (Fed. Cir. 1985).

Schneier, Ober, Arnold, Fischer, or any combination thereof fails to render claim 1 or claim 15 unpatentable under 35 U.S.C. § 103(a) because in order to establish a *prima facie* case of obviousness, all of the claimed limitations must be taught or suggested by the prior art, and there must be some suggestion or motivation, either in the references themselves or in the

knowledge generally available to one of ordinary skill in the art, to modify the references or to combine the reference teachings. *In re Vaek*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). The application of *Schneier, Ober, Arnold and Fischer* by the Office fails to meet this criteria, and claims 1 and 15 are allowable over *Schneier, Ober, Arnold and Fischer*.

2. Additional features of the invention recited in claim 1 are found in dependent claim 2.

Claim 2 recites that the processor internal to the module accesses the second super-root key only for decrypting encrypted root keys, wherein the decrypted root keys are then stored within the module inaccessible outside the secure module.

Claim 2 is allowable for at least the same reasons given above with respect to claim 1 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 2 under 35 U.S.C. § 103(a) as being unpatentable over *Schneier, Ober, Arnold and Fischer*.

3. Additional features of the invention recited in claim 2 are found in dependent claim 3.

Claim 3 recites that step (a) is performed in a corresponding secure module.

Claim 3 is allowable for at least the same reasons given above with respect to claim 2 and for the additional feature recited therein, and requests reconsideration and withdrawal of the rejection of claim 3 under 35 U.S.C. § 103(a) as being unpatentable over *Schneier, Ober, Arnold and Fischer*.

4. Additional features of the invention recited in claim 3 are found in dependent claim 4.

Claim 4 recites that the processor internal to the module accesses the second super-root key only in response to a request from a corresponding secure module.

Claim 4 is allowable for at least the same reasons given above with respect to claim 3 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 4 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

5. Additional features of the invention recited in claim 4 are found in dependent claim 5.

Claim 5 recites that the second super-root key and the first super-root key are the private and public portions of an asymmetric private/public-key pair, respectively.

Claim 5 is allowable for at least the same reasons given above with respect to claim 4 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 5 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

6. Additional features of the invention recited in claim 4 are found in dependent claim 6.

Claim 6 recites that the second super-root key and the first super-root key are a same private key for use with a symmetric key-based encryption algorithm.



Claim 6 is allowable for at least the same reasons given above with respect to claim 4 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 6 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

7. Additional features of the invention recited in claim 6 are found in dependent claim 7.

Claim 7 recites an additional step prior to step a) of a1) generating a first root key within a key-generating processor internal to the key provider system.

Claim 7 is allowable for at least the same reasons given above with respect to claim 6 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 7 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

8. Additional features of the invention recited in claim 7 are found in dependent claim 8.

Claim 8 recites that the key-generating processor is embodied on the corresponding secure module.

Claim 8 is allowable for at least the same reasons given above with respect to claim 7 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 8 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

9. Additional features of the invention recited in claim 6 are found in dependent claim 9.

Claim 9 recites that the first root key is useable for at least one of encrypting and decrypting private encryption keys.

Claim 9 is allowable for at least the same reasons given above with respect to claim 6 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 6 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

10. Additional features of the invention recited in claim 15 are found in dependent claim 16.

Claim 16 recites that the code executable on the encryption processor accesses the at least a first super-root key only in response to a request from a corresponding secure module.

Claim 16 is allowable for at least the same reasons given above with respect to claim 15 and for the additional feature recited therein, and Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 16 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

11. Additional features of the invention recited in claim 16 are found in dependent claim 17.

Claim 17 recites that the code executable on the encryption processor is only for performing encryption functions the results of which are inaccessible outside of the module.

Claim 17 is allowable for at least the same reasons given above with respect to claim 16 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 17 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

12. Additional features of the invention recited in claim 17 are found in dependent claim 18.

Claim 18 recites that the memory circuit for storing the at least a first super-root key is a read-only memory circuit.

Claim 18 is allowable for at least the same reasons given above with respect to claim 15 and for the additional feature recited therein, and Applicant requests reconsideration and withdrawal of the rejection of claim 18 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold and Fischer.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Spelman***

13. Claims 10-14 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423) and Spelman (U.S. Patent No. 5,680,458). Applicant respectfully traverses this rejection.

Amended claim 10 recites a method for transferring a first root key between a key provider system and a second other system via an information network. The method includes the steps of a) encrypting the first root key using a first super-root key of the key provider system; b) providing within the second other system a first secure module having second and third super-root keys within a memory circuit thereof, the second and third super-root keys accessible only by program code being executed on a processor internal to the first secure module for decrypting encrypted root keys and for storing the decrypted root keys within a memory circuit of the first secure module, and wherein the second and third super-root keys are other than accessible outside of the module; c) transferring the encrypted first root key from the key provider system to the second other system via the information network; d) providing the encrypted first root key to the processor internal to the first secure module of the second other system; and, e) executing program code on the processor internal to the first secure module to decrypt the encrypted first root key using the second super-root key stored within the memory circuit of the first secure module and to store the decrypted first root key internally within a secure key memory location of the first secure module, wherein the first root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first super-root key is greater than a bit length of the first root key, and the bit length of the first root key is greater than a bit length of any of the private keys.

Claim 10 is allowable for reasons analagous to those given for claims 1 and 15.

Further, Spelman describes a root key compromise recovery. Spelman fails to supplement the deficiencies of Schneier, Ober, Arnold and Fischer because Spelman fails to teach or reasonably suggest "encrypting the first root key using a first super-root key of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the first root key is useable for at least one of encrypting and decrypting private keys," as recited in claim 10.

14. Additional features of the invention recited in claim 10 are found in dependent claim 11.

Claim 11 recites the steps f) encrypting a fourth super-root key using one of the third super-root key and a key corresponding to the third super-root key; g) transferring the encrypted fourth super-root key from the key provider system to the second other system via the information network; h) providing the encrypted fourth super-root key to the processor internal to the first secure module of the second other system; and, i) executing program code on the processor internal to the first secure module to decrypt the encrypted fourth super-root key using the third super-root key stored within the memory circuit of the first secure module and to store the decrypted fourth super-root key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second super-root key was stored.

Claim 11 is allowable for at least the same reasons given above with respect to claim 10 and for the additional features recited therein, and Applicant respectfully requests

reconsideration and withdrawal of the rejection of claim 11 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer and Spelman.

15. Additional features of the invention recited in claim 11 are found in dependent claim 12.

Claim 12 recites that the second and third super-root keys are only replaceable through use of another of the second and third super-root keys.

Claim 12 is allowable for at least the same reasons given above with respect to claim 10 and for the additional features recited therein, and Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 12 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer and Spelman.

16. Additional features of the invention recited in claim 12 are found in dependent claim 13.

Claim 13 recites that the second, third and fourth super-root keys are useable for at least one of encrypting and decrypting root keys.

Claim 13 is allowable for at least the same reasons given above with respect to claim 10 and for the additional features recited therein, and Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 13 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer and Spelman.

17. Additional features of the invention recited in claim 11 are found in dependent claim 14.

Claim 14 recites that the step of storing the decrypted fourth super-root key comprises the steps of i1) erasing the second super-root key from a first storage area of the memory circuit; and, i2) storing the decrypted fourth super-root key within approximately the same first storage area of the same memory circuit.

Claim 14 is allowable for at least the same reasons given above with respect to claim 11 and for the additional features recited therein, and Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 14 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer and Spelman.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Easter***

18. Claim 19 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423) and Easter (U.S. Patent No. 5,598,889). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 18 are found in dependent claim 19.

Claim 19 recites that the module is FIPS 140 compliant.

Claim 19 is allowable for at least the same reasons given above with respect to claim 18 and for the additional features recited therein.

Further, Easter describes a system and method for data encryption using public key cryptology. Easter fails to supplement the deficiencies of Schneier, Arnold and Fischer because Fischer does not teach or reasonably suggest not teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 15.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 19 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer and Easter.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer and Bergum***

19. Claim 20 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Easter (U.S. Patent No. 5,598,889) and Bergum (U.S. Patent No. 5,249,277). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 19 are found in dependent claim 20.



Claim 20 recites that the module includes a tamper detection circuit for erasing the first super-root key in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

Claim 20 is allowable for at least the same reasons given above with respect to claim 19 and for the additional features recited therein.

Further, Bergum describes a method and apparatus of controlling processing devices during power transitions. Bergum fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer, and Easter because Bergum fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 15.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer, Easter and Bergum.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason and Ehram***

20. Claims 21-24 are rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S.

Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Spelman (U.S. Patent No. 5,680,458) and Mason (U.S. Patent No. 6,331,784). Applicant respectfully traverses this rejection.

Claim 21 recites a system for transferring a secure root key between a key provider system and a second other system via an information network that is other than secure comprising a secure module in operative communication with the second other system. The secure module includes an encryption processor, an input port, a memory circuit, and memory storage. The input port is for receiving encrypted electronic data from outside the module and for providing the encrypted electronic data to the encryption processor. The memory circuit is in operative communication with the encryption processor for storing a first super-root key within a first memory location thereof and for storing a second super-root key within a second other memory location thereof. The memory storage has program code stored therein and executable on the encryption processor for, upon receipt of an encrypted third super-root key from the second other system, decrypting the encrypted third super-root key using one of the first and second super-root keys and for storing the decrypted third super-root key at a memory location corresponding to the other one of the first and second super-root keys, the first and second super-root keys being accessible only by the program code and being modifiable only by the program code for all modifications excluding erasure, wherein the secure root key is useable for at least one of encrypting and decrypting private keys, and wherein a bit length of the first

super-root key is greater than a bit length of the secure root key, and the bit length of the secure root key is greater than a bit length of any of the private keys.

Claim 21 is allowable for reasons analagous to those given for claims 1, 10 and 15.

Further, Spelman describes a root key compromise recovery and Bergum describes a method and apparatus of controlling processing devices during power transitions. Spelman and Bergum fail to supplement the deficiencies of Schneier, Ober, Arnold and Fischer because Spelman and Bergum fail to teach or reasonably suggest "encrypting the **first root key** using a **first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 15.

21. Additional features of the invention recited in claim 21 are found in dependent claim 22.

Claim 22 recites that the code executable on the encryption processor accesses the first and second super-root keys only in response to a request from a corresponding secure module.

Claim 22 is allowable for at least the same reasons given above with respect to claim 21 and for the additional features recited therein, and Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 22 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer, Spelman and Mason.

22. Additional features of the invention recited in claim 22 are found in dependent claim 23.

Claim 23 recites that the code executable on the encryption processor is only for performing encryption functions the results of which are inaccessible outside of the module.

Claim 23 is allowable for at least the same reasons given above with respect to claim 22 and for the additional features recited therein, and Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 23 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer, Spelman and Mason.

23. Additional features of the invention recited in claim 23 are found in dependent claim 24.

Claim 24 recites that the memory circuit for storing the first and second super-root keys is a substantially non-volatile reprogrammable memory circuit.

Claim 24 is allowable for at least the same reasons given above with respect to claim 23 and for the additional features recited therein, and Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 24 under 35 U.S.C. § 103(a) as being unpatentable over Schneier, Ober, Arnold, Fischer, Spelman and Mason.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason, Ehram and Easter***

24. Claim 25 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423),

Spelman (U.S. Patent No. 5,680,458), Mason (U.S. Patent No. 6,331,784) and Ehram (U.S. Patent No. 4,386,234). Applicant respectfully traverses this rejection.

25. Additional features of the invention recited in claim 24 are found in dependent claim 25.

Claim 25 recites that the substantially non-volatile reprogrammable memory circuit is one of an electrically erasable programmable read-only memory (EEPROM) circuit and a random access memory (RAM) circuit having an on-board power supply in the form of a battery.

Claim 25 is allowable for at least the same reasons given above with respect to claim 24 and for the additional features recited therein.

Further, Ehram describes a cryptographic communication and file security using terminals. Ehram fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer, Spelman and Mason because Ehram fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 21.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 25 under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Ober, Arnold, Fischer, Spelman, Mason and Ehram.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason,  
Ehram and Easter***

26. Claim 26 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Spelman (U.S. Patent No. 5,680,458), Mason (U.S. Patent No. 6,331,784), Ehram (U.S. Patent No. 4,386,234) and Easter (U.S. Patent No. 5,598,889). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 25 are found in dependent claim 26.

Claim 26 recites that the module is FIPS 140 compliant.

Claim 26 is allowable for at least the same reasons given above with respect to claim 25 and for the additional features recited therein.

Further, Easter describes a system and method for data encryption using public key cryptography. Easter fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer, Spelman, Mason and Ehram because Easter fails to teach or reasonably suggest "encrypting the **first root key** using **a first super-root key** of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the **first root key** is useable for at least one of encrypting and decrypting **private keys**," as recited in claim 21.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 26 under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Ober, Arnold, Fischer, Spelman, Mason, Ehram and Easter.

***Rejection under 35 U.S.C. § 103(a) based on Schneier, Ober, Arnold, Fischer, Mason, Ehram, Easter and Bergum***

27. Claim 27 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Schneier (pages 166, 167, 176 and 177 of Applied Cryptography) in view of Ober (U.S. Patent No. 6,307,936), Arnold (U.S. Patent No. 6,175,924), Fischer (U.S. Patent No. 6,141,423), Spelman (U.S. Patent No. 5,680,458), Mason (U.S. Patent No. 6,331,784), Ehram (U.S. Patent No. 4,386,234), Easter (U.S. Patent No. 5,598,889) and Bergum (U.S. Patent No. 5,249,277). Applicant respectfully traverses this rejection.

Additional features of the invention recited in claim 26 are found in dependent claim 27.

Claim 27 recites that the module includes a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

Claim 27 is allowable for at least the same reasons given above with respect to claim 26 and for the additional features recited therein.

Further, Bergum describes a system and method for data encryption using public key cryptography. Bergum fails to supplement the deficiencies of Schneier, Ober, Arnold, Fischer,

Spelman, Mason, Ehram and Easter because Bergum fails to teach or reasonably suggest "encrypting the first root key using a first super-root key of the key provider," "transferring the encrypted first root key from the key provider system to the second other system via the information network," and "the first root key is useable for at least one of encrypting and decrypting private keys," as recited in claim 21.

Applicant respectfully requests reconsideration and withdrawal of the rejection of claim 27 under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Ober, Arnold, Fischer, Spelman, Mason, Ehram, Easter and Bergum.

#### *New Claims*

28. Newly added dependent claims 28-31 respectively depend from claims 1, 10, 15 and 21, and are allowable as being dependent from an allowable claim.

Further, each of these claims recites that the bit length of the first super-root key is within an approximate range of between 2048 bits and 4096 bits, the bit length of the first root key is within an approximate range of between 512 bits and 2048 bits, and the bit length of any of the private keys is within an approximate range of between 128 and 1024 bits

Applicant respectfully submits that Schneier, Ober, Arnold, Fischer, Spelman, Mason, Ehram, Easter, Bergum, or any combination thereof fails to teach or reasonably suggest these bit ranges.



### **Conclusion**

29. Applicant respectfully submits that the proposed amendments made herein properly respond to the outstanding Final Rejection and represent a *bona fide* effort to satisfactorily conclude the prosecution of this application. Care has been exercised to insure that no new matter has been introduced and that no new issues have been raised that would require further consideration or search. It is felt that no inordinate amount of time will be required on the part of the Examiner to review and consider this amendment. In the event that the application is not allowed, it is requested that this amendment be entered for purposes of appeal.

All of the stated grounds of rejection have been properly traversed. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

No additional fees are believed to be required. However, if the Office deems that any fees are necessary, authorization is hereby granted to charge any required fees to Deposit Account No. 22-0261.


Application No. 09/919,960  
Art Unit 2137

Docket No. 35997-215056  
Customer No. 26694

Prompt and favorable consideration of this Amendment is respectfully requested.

March 28, 2006

Respectfully submitted,

By   
\_\_\_\_\_  
James R. Burdett  
Registration No. 31,594  
Thomas C. Schoeffler  
Registration No. 43,385  
VENABLE LLP  
P.O. Box 34385  
Washington, DC 20043-9998  
Attorney/Agent for Applicant

MAS/TCS